日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　１月１１日

出願番号
Application Number: 特願２００１－００３４６７

出願人
Applicant(s): 沖電気工業株式会社

ONISHI
31869-174125
8-9-01

２００１年　５月１８日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

CERTIFIED COPY OF
PRIORITY DOCUMENT

出証番号　出証特２００１－３０４１２６９

【書類名】　特許願
【整理番号】　MA001307
【提出日】　平成13年 1月11日
【あて先】　特許庁長官殿
【国際特許分類】　G09C 1/00 630
【発明者】
【住所又は居所】　東京都港区虎ノ門１丁目７番１２号　沖電気工業株式会社内
【氏名】　大西　一三
【特許出願人】
【識別番号】　000000295
【氏名又は名称】　沖電気工業株式会社
【代表者】　篠塚　勝正
【代理人】
【識別番号】　100083840
【弁理士】
【氏名又は名称】　前田　実
【手数料の表示】
【予納台帳番号】　007205
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9003703
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　間欠信号の暗号化伝送システム

【特許請求の範囲】

【請求項１】　第１通信装置から第２通信装置に間欠信号を伝送する際に、第１通信装置では、内部に備えられた暗号化回路で該間欠信号に対して暗号化を実施してから送信回路で送出し、第２通信装置では、内部に備えられた受信回路で受信した前記間欠信号を復号化回路で復号する暗号化伝送システムであって、

前記第１通信装置は、暗号化前の第１の間欠信号に基づいて第２の間欠信号用の送信側秘話鍵を生成する送信側秘話鍵生成回路と、該送信側秘話鍵を第２の間欠信号の暗号化に用いるために遅延させる送信側メモリとを有し、

前記第２通信装置は、復号化後の第１の間欠信号に基づいて第２の間欠信号用の受信側秘話鍵を生成する受信側秘話鍵生成回路と、該受信側秘話鍵を第２の間欠信号の暗号化に用いるために遅延させる受信側メモリとを有することを特徴とする暗号化伝送システム。

【請求項２】　前記第２通信装置は、前記受信回路から出力される復号前の前記間欠信号中の伝送エラーを検出して、秘話初期化制御用の間欠信号を生成する初期化制御信号生成回路と、該秘話初期化制御用の間欠信号を第１通信装置に送出できる送信回路とを有し、

前記第１通信装置は、前記秘話初期化制御用の間欠信号を受信した場合、前記送信側秘話鍵生成回路、送信側メモリ、および、暗号化回路に対して初期化信号を送出する受信回路を有することを特徴とする請求項１に記載の暗号化伝送システム。

【請求項３】　前記第１通信装置は、暗号化前の間欠信号に対してスクランブル処理を施すスクランブル回路と、該スクランブル回路に供給する擬似ランダムパタンを発生させる擬似ランダムパタン発生回路とを有し、

前記第２通信装置は、復号化後の間欠信号に対してデスクランブル処理を施すデスクランブル回路と、該デスクランブル回路に供給する擬似ランダムパタンを発生させる擬似ランダムパタン発生回路とを有することを特徴とする請求項１または２に記載の暗号化伝送システム。

【請求項４】　前記第１通信装置および前記第２通信装置は、無線方式あるいは有線方式で双方向に間欠信号を伝送でき、第２通信装置は、前記第１通信装置と同様に暗号化回路、送信回路、送信側秘話鍵生成回路、および、送信側メモリを備え、第１通信装置は、前記第２通信装置と同様に受信回路、復号化回路、受信側秘話鍵生成回路、および、受信側メモリを備えることを特徴とする請求項１～３の何れかに記載の暗号化伝送システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、複数の通信装置が各通信装置間において信号を伝送する際に暗号化を実施する暗号化伝送システムに関し、特に、パケット通信方式のような間欠信号を各通信装置間において伝送する際に暗号化を実施できる暗号化伝送システムに関する。

【０００２】

【従来の技術】

従来の秘話通信を実施する暗号化伝送システムは、以下のように構成される。

【０００３】

図８は、従来の暗号化伝送システムの概略構成を示す図である。

【０００４】

第１通信装置２２０と第２通信装置２８０とは伝送路３００により通信接続されている。伝送路３００は、銅線あるいは光ファイバ等の有線接続と、電波あるいは赤外線等の無線接続の双方を含む伝送路である。

【０００５】

第１通信装置２２０は、大きく分けて送信側回路と受信側回路とに分かれており、送信側回路には、送信信号Ａを例えば符号の順序入れ替え等の手法によりスクランブル化してスクランブル信号ＣＡを出力するスクランブル回路２２１と、そのスクランブル回路２２１に擬似ランダムパタンＲＡ１を供給する擬似ランダムパタン発生回路２２２と、スクランブル信号ＣＡをさらに変調させた変調信号ＭＣＡとして送信する送信回路２２３とを有している。

【０００６】

一方、第１通信装置２２０の受信側回路には、受信した変調信号ＭＣＢを復調させてスクランブル信号ＣＢを出力する受信回路２３０と、スクランブル信号ＣＢをデスクランブル化した受信信号Ｂとして出力するデスクランブル回路２３１と、そのデスクランブル回路２３１に擬似ランダムパタンＲＡ２を供給する擬似ランダムパタン発生回路２３２とを有している。

【０００７】

第２通信装置２８０も、第１の通信装置２２０と同様に、大きく分けて送信側回路と受信側回路とに分かれており、送信側回路には、送信信号Ｂをスクランブル化してスクランブル信号ＣＢを出力するスクランブル回路２８１と、そのスクランブル回路２８１に擬似ランダムパタンＲＡ２を供給する擬似ランダムパタン発生回路２８２と、スクランブル信号ＣＢをさらに変調させた変調信号ＭＣＢとして送信する送信回路２８３とを有し、第２通信装置２８０の受信側回路には、受信した変調信号ＭＣＡを復調させてスクランブル信号ＣＡを出力する受信回路２９０と、スクランブル信号ＣＡをデスクランブル化した受信信号Ａとして出力するデスクランブル回路２９１と、そのデスクランブル回路２９１に擬似ランダムパタンＲＡ１を供給する擬似ランダムパタン発生回路２９２とを有している。

【０００８】

上記のように図８の第１通信装置２２０および第２通信装置２８０には、各々送信回路および受信回路を備えて双方向送受信が可能な構成を有しているが、一方向の送受信は逆方向の送受信と符号が異なるのみであるので、以下に記載する図８の暗号化伝送システムの動作の説明では、第１通信装置２２０から信号Ａを第２通信装置２８０へ送信する場合のみを記載し、逆方向への信号Ｂの送信については記載を省略する。

【０００９】

第１通信装置２２０において、信号Ａがスクランブル回路２２１に入力されると、スクランブル回路２２１では、擬似ランダムパタン発生回路２２２から入力される擬似ランダムパタンＲＡ１により信号Ａに対するスクランブル化が実施され、スクランブル信号ＣＡが出力される。

【００１０】

スクランブル信号ＣＡが送信回路２２３に入力されると、送信回路２２３では、スクランブル信号ＣＡに対して送信信号とするための変調が実施され、変調信号ＭＣＡが伝送路３００に出力される。

【００１１】

伝送路３００から第２通信回路２８０に変調信号ＭＣＡが入力されると、受信回路２９０では、変調信号ＭＣＡが復調されてスクランブル信号ＣＡが出力される。

【００１２】

スクランブル信号ＣＡがデスクランブル回路２９１に入力されると、デスクランブル回路２９１では、擬似ランダムパタン発生回路２９２から入力される擬似ランダムパタンＲＡ１により信号Ａに対するデスクランブル化が実施され、復号された信号Ａが出力される。

【００１３】

ところが、図８に示した従来の暗号化伝送システムでは、ランダムパターンが固定であり、変換規則および変換周期等を同仕様で多数の通信装置を制作した場合には、第３者の解読可能性を０に近づけて秘話性を高めようとすると、長い擬似ランダムパターンＲＡ１を用いることになる。すると、回路規模が増大してコストも増加するという問題がある。その問題を解決するために、例えば、特開平05-007202号公報に記載されたように、簡単な構成で秘話性も高い暗号化伝送システムが知られている。

【００１４】

図９は、特開平05-007202号公報に記載された従来の暗号化伝送システムの概略構成を示す図である。

【００１５】

図９の暗号化伝送システムでは、例えば、図８の暗号化伝送システムにおける擬似ランダムパタン発生回路２２２および２９２等を無くし、代わりに受信信号を暗号化のための鍵情報として用いるように構成している。

【００１６】

第１通信装置２００は、その送信側回路側に、受信した信号Ｂ’から得られた鍵信号を用いて送信する信号Ａを暗号化して暗号化信号ＣＡを出力する変換部２０１と、暗号化信号ＣＡをさらに変調させた変調信号ＭＣＡとして送信する送信回路２０３とを有している。また、受信側回路側には、受信した変調信号ＭＣＢを復調させて暗号化信号ＣＢを出力する受信回路２１０と、暗号化信号ＣＢを逆変換した信号Ｂ’として出力する逆変換部２１１と、その逆変換部２１１に逆変換用の鍵情報として格納しておいた信号Ａを供給するメモリ２０２とを有している。メモリ２０２には、送信する信号Ａが変換部２０１に入力される時に、信号Ａが並列に入力されて格納される。

【００１７】

第２通信装置２６０は、第１通信装置２００と同様に、送信側回路側に、受信した信号Ａ’から得られた鍵信号を用いて送信する信号Ｂを暗号化して暗号化信号ＣＢを出力する変換部２６１と、暗号化信号ＣＢをさらに変調させた変調信号ＭＣＢとして送信する送信回路２６３とを有しており、受信側回路側には、受信した変調信号ＭＣＡを復調させて暗号化信号ＣＡを出力する受信回路２７０と、暗号化信号ＣＡを逆変換した信号Ａ’として出力する逆変換部２７１と、その逆変換部２７１に逆変換用の鍵情報として格納しておいた信号Ｂを供給するメモリ２６２とを有している。メモリ２６２には、送信する信号Ｂが変換部２６１に入力される時に、信号Ｂが並列に入力されて格納される。

【００１８】

図９の暗号化伝送システムでは、上記のように、送信信号Ａについては受信信号Ｂ’を鍵情報として利用し、且つ、受信した暗号化信号ＣＢを逆変換するためには、送信した信号Ａを利用しているので、簡単な構成で高い秘話性を得ることができる。

【００１９】

【発明が解決しようとする課題】

しかしながら、上記した図９の従来の暗号化伝送システムでは、受信した暗号化信号ＣＢを逆変換するために送信した信号Ａを利用しているので、送信信号と受信信号の連続性が途切れると、逆変換するための鍵情報が変換時の鍵情報と一

致しなくなるので、暗号化伝送ができなくなるという問題があった。

【００２０】

すなわち、信号Ａを第１通信装置２００から送信した場合、第２通信装置２６０では信号Ｂを送信するために受信した信号Ａ’を鍵情報として用いて変換した暗号化信号ＣＢとしてから送信し、第１通信装置２００では受信した暗号化信号ＣＢをメモリに格納しておいた信号Ａを鍵情報として逆変換するが、信号Ａが、例えば、Ａ１、Ａ２、Ａ３、・・・のように連続して間断なく出力されないと、第１通信装置２００のメモリ２０２に格納しておいた信号Ａと、第２通信装置２６０で鍵情報として利用した信号Ａ’が一致しなくなり、その結果、暗号化した信号を元に戻せなくなり、秘話通信ができなくなるという問題があった。

【００２１】

上記のように、図９の暗号化伝送システムは、信号Ａが間断なく出力されないと秘話通信できなくなるので、例えば、ＩＰ（インターネット・プロトコル）パケット伝送のような間欠的にデータが流れる伝送経路では用いることができなかった。

【００２２】

本発明は、上述した如き従来の問題を解決するためになされたものであって、ＩＰパケット伝送のような間欠的にデータが流れる伝送経路でも暗号化した通信を実施できる簡単な構成の暗号化伝送システムを提供することを目的とする。

【００２３】

【課題を解決するための手段】

上述の目的を達成するため、請求項１に記載した本発明の暗号化伝送システムは、第１通信装置から第２通信装置に間欠信号を伝送する際に、第１通信装置では、内部に備えられた暗号化回路で該間欠信号に対して暗号化を実施してから送信回路で送出し、第２通信装置では、内部に備えられた受信回路で受信した間欠信号を復号化回路で復号する暗号化伝送システムであって、第１通信装置は、暗号化前の第１の間欠信号に基づいて第２の間欠信号用の送信側秘話鍵を生成する送信側秘話鍵生成回路と、該送信側秘話鍵を第２の間欠信号の暗号化に用いるために遅延させる送信側メモリとを有し、第２通信装置は、復号化後の第１の間欠

信号に基づいて第２の間欠信号用の受信側秘話鍵を生成する受信側秘話鍵生成回路と、該受信側秘話鍵を第２の間欠信号の暗号化に用いるために遅延させる受信側メモリとを有することを特徴とする。

【００２４】

また、請求項２の本発明は、請求項１に記載の暗号化伝送システムにおいて、第２通信装置は、受信回路から出力される復号前の間欠信号中の伝送エラーを検出して、秘話初期化制御用の間欠信号を生成する初期化制御信号生成回路と、該秘話初期化制御用の間欠信号を第１通信装置に送出できる送信回路とを有し、第１通信装置は、秘話初期化制御用の間欠信号を受信した場合、送信側秘話鍵生成回路、送信側メモリ、および、暗号化回路に対して初期化信号を送出する受信回路を有することを特徴とする。

【００２５】

また、請求項３の本発明は、請求項１または２に記載の暗号化伝送システムにおいて、第１通信装置は、暗号化前の間欠信号に対してスクランブル処理を施すスクランブル回路と、該スクランブル回路に供給する擬似ランダムパタンを発生させる擬似ランダムパタン発生回路とを有し、第２通信装置は、復号化後の間欠信号に対してデスクランブル処理を施すデスクランブル回路と、該デスクランブル回路に供給する擬似ランダムパタンを発生させる擬似ランダムパタン発生回路とを有することを特徴とする。

【００２６】

また、請求項４の本発明は、請求項１～３の何れかに記載の暗号化伝送システムにおいて、第１通信装置および第２通信装置は、無線方式あるいは有線方式で双方向に間欠信号を伝送でき、第２通信装置は、第１通信装置と同様に暗号化回路、送信回路、送信側秘話鍵生成回路、および、送信側メモリを備え、第１通信装置は、第２通信装置と同様に受信回路、復号化回路、受信側秘話鍵生成回路、および、受信側メモリを備えることを特徴とする。

【００２７】

【発明の実施の形態】

以下、本発明を図示した実施形態に基づいて説明する。

【００２８】

図１は、本発明の第１の実施形態の暗号化伝送システムの構成を示すブロック図である。また、図１中で図８及び図９に示した従来の暗号化システムと同じ機能の部分については、図８または図９と同じ符号を用いて重複する記載を省略する。

【００２９】

第１通信装置１は、暗号化送信部１０と受信復号部２０とに分かれており、暗号化送信部１０には、間欠信号の一種であるパケット信号で構成される送信信号Ａを例えば符号の順序入れ替え等の手法により暗号化して暗号化信号ＣＡを出力する暗号化回路１１と、パケット信号の暗号化信号ＣＡをさらに変調させた変調信号ＭＣＡとして送信する送信回路１２と、暗号化回路１１に供給するための秘話鍵ＫＡをパケット信号の送信信号Ａから生成する秘話鍵生成回路１３と、前回のパケット信号である送信信号Ａにより秘話鍵生成回路１３で生成された秘話鍵ＫＡを次回のパケット信号を暗号化させるために格納して遅延させるメモリ１４とを有している。

【００３０】

一方、第１通信装置１の受信復号部２０には、受信した変調信号ＭＣＢを復調させて暗号化信号ＣＢを出力する受信回路２１と、暗号化信号ＣＢを復号化した受信信号Ｂ’として出力する復号化回路２２と、その復号化回路２２に供給するための秘話鍵ＫＢをパケット信号である受信信号Ｂ’から生成する秘話鍵生成回路２３と、前回のパケット信号である受信信号Ｂ’により秘話鍵生成回路２３で生成された秘話鍵ＫＢを次回のパケット信号を暗号化させるために格納して遅延させるメモリ２４とを有している。

【００３１】

第２通信装置６も、第１の通信装置１と同様に、大きく分けて暗号化送信部７０と受信復号部６０とに分かれており、暗号化送信部７０には、送信信号Ｂを暗号化して暗号化信号ＣＢを出力する暗号化回路７１と、パケット信号である暗号化信号ＣＢをさらに変調させた変調信号ＭＣＢとして送信する送信回路７２と、暗号化回路７１に供給するための秘話鍵ＫＢをパケット信号である送信信号Ｂか

ら生成する秘話鍵生成回路７３と、前回のパケット信号である送信信号Ｂにより秘話鍵生成回路７３で生成された秘話鍵ＫＢを次の回のパケット信号を暗号化させるために格納して遅延させるメモリ７４とを有し、第２通信装置６の受信復号部６０には、受信した変調信号ＭＣＡを復調させて暗号化信号ＣＡを出力する受信回路６１と、暗号化信号ＣＡを復号化した受信信号Ａ’として出力する復号化回路６２と、その復号化回路６２に供給するための秘話鍵ＫＡをパケット信号である受信信号Ａ’から生成する秘話鍵生成回路６３と、前回のパケット信号である受信信号Ａ’により秘話鍵生成回路６３で生成された秘話鍵ＫＡを次回のパケット信号を暗号化させるために格納して遅延させるメモリ６４とを有している。

【００３２】

上記のように図１の第１通信装置１および第２通信装置６には、各々暗号化送信部１０、７０回路および受信復号部２０，６０を備えて双方向送受信が可能な構成を有しているが、例えば、暗号化送信部１０から受信復号部６０への方向の送受信は、暗号化送信部７０から受信復号部２０への逆方向の送受信と符号が異なるのみである。そこで、以下に記載する図１の暗号化伝送システムの動作の説明では、図１から一方向の送受信に関するブロックのみを抜き出した図２に示したように、第１通信装置１から信号Ａを第２通信装置６へ送信する場合のみを記載し、逆方向への信号Ｂの送信については記載を省略する。

【００３３】

図３（ａ）は、図１の第１通信装置１に入力されるパケット信号の送信信号Ａを時系列に示した図であり、図３（ｂ）は、図１の第１通信装置１中の暗号化回路１１から出力されるパケット信号の暗号化信号ＣＡを時系列に示した図であり、図３（ｃ）は、図１の第２通信装置６から出力されるパケット信号の受信信号Ａ’を時系列に示した図である。

【００３４】

第１通信装置１において、最初にパケット信号の信号Ａが暗号化回路１１に入力されると、暗号化回路１１では、メモリ１４から入力される遅延された秘話鍵ＤＫＡにより信号Ａに対する暗号化が実施され、暗号化信号ＣＡが出力される。

【００３５】

〔信号Ａ（ｎ－２）の入力時：（ｎは３以上の正の整数）〕

例えば、図３（ａ）に示したように、最初に信号Ａ（ｎ－２）が暗号化回路１１に入力された場合について説明する。信号Ａ（ｎ－２）は、暗号化回路１１で、メモリ１４に格納されていた初期値（例えばオール０等）により暗号化されて、図３（ｂ）に示したように暗号化信号ＣＡ（ｎ－２）が出力される。また、上記の処理と平行して信号Ａ（ｎ－２）は秘話鍵生成回路１３にも入力され、秘話鍵生成回路１３では秘話鍵ＫＡ（ｎ－２）が生成されてメモリ１４に格納される。暗号化信号ＣＡ（ｎ－２）は送信回路１２で変調信号ＭＣＡ（ｎ－２）に変調されて第２通信装置６に送出される。

【００３６】

第２通信装置６の受信回路６１は、変調信号ＭＣＡ（ｎ－２）を受信すると復調を実施して暗号化信号ＣＡ（ｎ－２）を復号化回路６２に出力する。復号化回路６２では、暗号化信号ＣＡ（ｎ－２）に対して、メモリ６４に格納されていた初期値（例えばオール０等）を用いて復号化を実施し、図３（ｃ）に示したように信号Ａ’（ｎ－２）を出力する。信号Ａ’（ｎ－２）は第２通信装置６から外部に出力されると同時に秘話鍵生成回路６３にも入力される。秘話鍵生成回路６３では信号Ａ’（ｎ－２）に基づいて秘話鍵ＫＡ（ｎ－２）が生成されてメモリ６４に格納される。

【００３７】

〔信号Ａ（ｎ－１）の入力時：〕

図３（ａ）に示したように、信号Ａ（ｎ－２）の次に信号Ａ（ｎ－１）が暗号化回路１１に入力された場合について説明する。信号Ａ（ｎ－１）は、暗号化回路１１で、メモリ１４に格納されていた秘話鍵ＤＫＡ（ｎ－２）により暗号化されて、図３（ｂ）に示したように暗号化信号ＣＡ（ｎ－１）が出力される。また、上記の処理と平行して信号Ａ（ｎ－１）は秘話鍵生成回路１３にも入力され、秘話鍵生成回路１３では秘話鍵ＫＡ（ｎ－１）が生成されてメモリ１４に格納される。暗号化信号ＣＡ（ｎ－１）は送信回路１２で変調信号ＭＣＡ（ｎ－１）に変調されて第２通信装置６に送出される。

【００３８】

第２通信装置６の受信回路６１は、変調信号ＭＣＡ（ｎ－１）を受信すると復調を実施して暗号化信号ＣＡ（ｎ－１）を復号化回路６２に出力する。復号化回路６２では、暗号化信号ＣＡ（ｎ－１）に対して、メモリ６４に格納されていた秘話鍵ＤＫＡ（ｎ－２）を用いて復号化を実施し、図３（ｃ）に示したように信号Ａ’（ｎ－１）を出力する。信号Ａ’（ｎ－１）は第２通信装置６から外部に出力されると同時に秘話鍵生成回路６３にも入力される。秘話鍵生成回路６３では信号Ａ’（ｎ－１）に基づいて秘話鍵ＫＡ（ｎ－１）が生成されてメモリ６４に格納される。

【００３９】

｛信号Ａ（ｎ）の入力時：｝

図３（ａ）に示したように、信号Ａ（ｎ－２）、信号Ａ（ｎ－１）に続いて信号Ａ（ｎ）が暗号化回路１１に入力された場合について説明する。信号Ａ（ｎ）は、暗号化回路１１で、メモリ１４に格納されていた秘話鍵ＤＫＡ（ｎ－１）により暗号化されて、図３（ｂ）に示したように暗号化信号ＣＡ（ｎ）が出力される。また、上記の処理と平行して信号Ａ（ｎ）は秘話鍵生成回路１３にも入力され、秘話鍵生成回路１３では秘話鍵ＫＡ（ｎ）が生成されてメモリ１４に格納される。暗号化信号ＣＡ（ｎ）は送信回路１２で変調信号ＭＣＡ（ｎ）に変調されて第２通信装置６に送出される。

【００４０】

第２通信装置６の受信回路６１は、変調信号ＭＣＡ（ｎ）を受信すると復調を実施して暗号化信号ＣＡ（ｎ）を復号化回路６２に出力する。復号化回路６２では、暗号化信号ＣＡ（ｎ）に対して、メモリ６４に格納されていた秘話鍵ＤＫＡ（ｎ－１）を用いて復号化を実施し、図３（ｃ）に示したように信号Ａ’（ｎ）を出力する。信号Ａ’（ｎ）は第２通信装置６から外部に出力されると同時に秘話鍵生成回路６３にも入力される。秘話鍵生成回路６３では信号Ａ’（ｎ）に基づいて秘話鍵ＫＡ（ｎ）が生成されてメモリ６４に格納される。

【００４１】

｛信号Ａ（ｎ＋１）の入力時：｝

上記と同様にして、第１通信装置１の暗号化回路１１に信号Ａ（ｎ＋１）が入

力されると、秘話鍵ＤＫＡ（ｎ）による暗号化が実施されて暗号化信号ＣＡ（ｎ＋１）が送出される。また第２通信装置６の復号化回路６２に暗号化信号ＣＡ（ｎ＋１）が入力されると、秘話鍵ＤＫＡ（ｎ）による復号化が実施されて信号Ａ’（ｎ＋１）が出力される。

【００４２】

このように、本実施形態では、送信側で１つ前のパケット信号から生成された秘話鍵を用いて次のパケット信号の暗号化を実施し、受信側でも１つ前のパケット信号から生成された秘話鍵を用いて次のパケット信号の復号化を実施するように構成したので、簡単な構成でも秘話鍵が順次変化することから第３者が解読することが困難であり、パケット伝送のような間欠的にデータが流れる伝送経路でも暗号化した通信を実施することができる。

【００４３】

ところで、上記した第１の実施形態では、第１通信装置１から送信したパケット信号が伝送経路の異常等により第２通信装置６に正常に届かない場合には、次のパケット信号の秘話鍵が送信側と受信側で一致しなくなるので、以後の暗号化通信ができなくなるという問題があった。そこで、次の第２の実施形態では、伝送経路等に異常が発生した場合に、第１通信装置１および第２通信装置６を初期化して再度暗号化通信を再開できる暗号化伝送システムについて説明する。

【００４４】

図４は、本発明の第２の実施形態の暗号化伝送システムの構成を示すブロック図である。

【００４５】

図４に示した第２の実施形態と図１に示した第１の実施形態との違いは、主に第１通信装置２および第２通信装置７内に、相対する各通信装置の暗号化回路等を初期化するための初期化制御信号ＩＰＡ、ＩＰＢを生成するための回路（初期化生成回路３５、９５）を有している点、その初期化制御信号ＩＰＡ、ＩＰＢを相対する通信装置内の暗号化送信部３０、９０に向けて送出することにより、暗号化回路３１、９１、秘話鍵生成回路３３、９３、メモリ３４、９４、を初期化できる点である。

【００４６】

図４の第１通信装置２および第２通信装置７には、上記のように、各々暗号化送信部３０、９０回路および受信復号部４０，８０を備えて双方向送受信が可能な構成を有しているが、例えば、暗号化送信部３０から受信復号部８０の方向への送受信は、暗号化送信部９０から受信復号部４０への逆方向の送受信と符号が異なるのみである。そこで、以下に記載する図４の暗号化伝送システムの動作の説明では、図４から一方向の送受信に関するブロックのみを抜き出した図５に示したように、第１通信装置２から信号Ａを第２通信装置７へ送信する場合のみを記載し、逆方向への信号Ｂの送信については記載を省略する。

【００４７】

図６（ａ）は、図５の第１通信装置２に入力されるパケット信号の送信信号Ａが暗号化されて送信され、正常に第２通信装置７に受信されて復号化される場合のフローチャートであり、図６（ｂ）は、図５の第１通信装置２から暗号化されて送信されたパケット信号の送信信号Ａに伝送エラー（異常）が発生し、第２通信装置７で正常に受信できなかった場合のフローチャートである。

【００４８】

図６（ａ）の場合、すなわち、第１通信装置２から第２通信装置７に暗号化された信号が正常に（伝送エラーが無く）届いて、正常な復号が可能な場合には、上記した第１の実施形態と同様に、第１通信装置側で、前回のパケット信号から生成された秘話鍵により送信信号に暗号化処理が実施されて送出される（ステップＳ１）。また、第２通信装置側では、前回のパケット信号から生成された秘話鍵により受信信号に復号化処理（ステップＳ２）が実施される。

【００４９】

図６（ｂ）の場合、すなわち、伝送エラーが発生する場合には、まず、第１通信装置側で、前回のパケット信号から生成された秘話鍵により送信信号に暗号化処理が実施されて送出されると（ステップＳ１１）、第２通信装置側では、受信回路８１で、受信したパケット信号の変調信号ＭＣＡからフレーム・チェック・シーケンス（ＦＣＳ）を検出することにより伝送エラーが発生したことを検知する（ステップＳ１２）。ＦＣＳエラーを検出した受信回路８１は、伝送エラーが

発生したことを示すエラー信号ＥＤＡを初期化制御信号生成回路９５に送信する。エラー信号ＥＤＡを受信した初期化制御信号生成回路９５では、第１通信装置２内の暗号化送信部３０を初期化する保守用の初期化制御信号ＩＰＡ（パケット信号）を生成し、その初期化制御信号ＩＰＡを送信回路９２により第１通信装置２へ向けて送出する（ステップＳ１３）。

【００５０】

初期化制御信号ＩＰＡを受信した第１通信装置２内の受信回路４１では、その初期化制御信号ＩＰＡの受信をトリガとして、暗号化送信部３０を初期化するための初期化指示信号ＩＣＡを暗号化回路３１、秘話鍵生成回路３３、および、メモリ３４に向けて送出する。受信回路４１は、ステップＳ１４の処理を実施するとともに、初期化制御信号ＩＰＡを正常に受信したことを示すＩＰＡ正常受信信号ＲＩＡを初期化制御信号生成回路３５に出力する。ＩＰＡ正常受信信号ＲＩＡを受信した初期化制御信号生成回路３５では、第２通信装置２内の受信復号部８０を初期化する保守用の初期化応答信号ＩＲＡ（パケット信号）を生成し、その初期化応答信号ＩＲＡを送信回路３２により第２通信装置７へ向けて送出する（ステップＳ１４）。

【００５１】

初期化応答信号ＩＲＡを受信した第２通信装置７内の受信回路８１では、その初期化応答信号ＩＲＡの受信をトリガとして、受信復号部８０を初期化するための初期化指示信号ＲＣＡを復号化回路８２、秘話鍵生成回路８３、および、メモリ８４に向けて送出する（ステップＳ１５）。

【００５２】

初期化された第１通信装置２内の暗号化送信部３０では、メモリ３４が初期値（例えば、オール０等）となる。従って、暗号化回路３１では、秘話鍵の初期値から暗号化を開始する（ステップＳ１６）。この初期値により暗号化された変調信号ＭＣＡが第１通信装置２から第２通信装置７に送出される。

【００５３】

第２通信装置７内の受信復号部８０では、初期値により暗号化された変調信号ＭＣＡが受信回路８１で受信されると、秘話鍵の初期値から復号化を開始する（

ステップＳ１７）。以後は、上記した第１の実施形態と同様に、第１通信装置２側で、前回のパケット信号から生成された秘話鍵により送信信号に暗号化処理が実施されて送出され（ステップＳ１８）、第２通信装置側では、前回のパケット信号から生成された秘話鍵により受信信号に復号化処理（ステップＳ１９）が実施される。

【００５４】

このように、本実施形態では、伝送エラー等により第１通信装置から送出されたパケット信号が正常に第２通信装置で受信されなかった場合には、初期化制御信号および初期化応答信号により第１通信装置の暗号化送信部と第２通信装置の受信復号部を初期化できるように構成したので、第１の実施形態と同様に、簡単な構成でも秘話鍵が順次変化することから第３者が解読することが困難であり、パケット伝送のような間欠的にデータが流れる伝送経路でも暗号化した通信を実施することができることに加えて、間欠的にデータが流れる伝送経路で伝送エラーが発生する場合でも、暗号化した通信を実施することができる。

【００５５】

ところで、上記した第１の実施形態では、通信開始時には秘話鍵の初期値としてオール０等の固定値を用いることから、最初から傍受する第３者に対して暗号解読のための手がかりを与えてしまう可能性があり、第２の実施形態では、通信開始時に加えて、通信中の伝送エラーによる初期化時にも傍受する第３者に対して暗号解読のための手がかりを与えてしまう可能性がある。そこで、次の第３の実施形態では、通信開始時および通信中の初期化時にも、第３者に対して暗号解読のための手がかりを与えにくい暗号化伝送システムについて説明する。

【００５６】

図７は、本発明の第３の実施形態の暗号化伝送システムの構成を示すブロック図である。

【００５７】

図７に示した第３の実施形態と図１に示した第１の実施形態との違いは、主に第１通信装置３内に送信する信号Ａを事前にスクランブル処理してスクランブル信号ＳＡを出力するスクランブル回路５６と、そのスクランブル回路５６に擬似

ランダムパターンＲＡを供給する擬似ランダムパターン発生回路５５とを有し、第２通信装置８内に、復号化したスクランブル信号ＳＡをデスクランブル処理するデスクランブル回路１０６と、そのデスクランブル回路１０６に擬似ランダムパターンＲＡを供給する擬似ランダムパターン発生回路１０５とを有している点である。

【００５８】

そのため、第１通信装置３の暗号化回路５１では、スクランブル信号ＳＡに対してさらに暗号化処理を実施した暗号化信号ＣＳＡを出力するようになり、送信回路５２では、暗号化信号ＣＳＡに対して変調を実施した変調信号ＭＣＳＡを出力する。また、秘話鍵生成回路５３は、スクランブル信号ＳＡに基づいて秘話鍵ＫＳＡを生成し、メモリ５４は、秘話鍵ＫＳＡを格納することにより次のパケット信号が入力するまで遅延させた秘話鍵ＤＫＳＡを出力する。

【００５９】

また、第２通信装置８の受信回路１０１は、受信した変調信号ＭＣＳＡを復調して暗号化信号ＣＳＡを出力し、復号化回路１０２は、暗号化信号ＣＳＡを受信すると、その信号を復号してスクランブル信号ＳＡを出力する。また、スクランブル信号ＳＡは秘話鍵生成回路１０３にも入力される。秘話鍵生成回路１０３では、入力したスクランブル信号ＳＡに基づいて秘話鍵ＫＳＡを生成し、メモリ１０４は、秘話鍵ＫＳＡを格納することにより次の暗号化信号ＣＳＡが入力するまで遅延させた秘話鍵ＤＫＳＡを出力する。

【００６０】

なお、図７に示した第３の実施形態は、図１に示した第１の実施形態にスクランブル回路等を付加したものであるが、同様にして図４に示した第２の実施形態に対してもスクランブル回路等を付加することができる。

【００６１】

このように、本実施形態では、通信開始時や通信中の伝送エラーによる初期化時に、最初からスクランブル処理された信号を用いるようにしたので、第１の実施形態と同様に、簡単な構成でも秘話鍵が順次変化することから第３者が解読することが困難であり、パケット伝送のような間欠的にデータが流れる伝送経路で

も暗号化した通信を実施することができること、および、第２の実施形態と同様に、間欠的にデータが流れる伝送経路で伝送エラーが発生する場合でも、暗号化した通信を実施することができることに加えて、最初から傍受する第３者に対して暗号解読のための手がかりを与えてしまう可能性を減らすことができる。

【００６２】

なお、上記した各実施形態では、第１通信装置と第２通信装置との間の伝送として説明したが、本発明はこれに限られるものではなく、例えば、２個以上の複数の通信装置を接続するネットワーク中から任意の２つの通信装置間でパケット信号のような間欠信号の送受信が実施される場合にも適用することができる。

【００６３】

【発明の効果】

上記のように本発明では、通信開始時や通信中の伝送エラーによる初期化時に、最初からスクランブル処理された信号を用いるようにし、簡単な構成でも秘話鍵が順次変化するので、第３者が解読することが困難であることに加えて、パケット伝送のような間欠的にデータが流れる伝送経路でも暗号化した通信を実施することができる。

【００６４】

また、本発明では、上記した効果に加えて、間欠的にデータが流れる伝送経路で伝送エラーが発生する場合であっても、暗号化した通信を実施することができる。

【００６５】

また、本発明では、上記した効果に加えて、最初から傍受する第３者に対して暗号解読のための手がかりを与えてしまう可能性を減らすことができる。

【図面の簡単な説明】

【図１】　本発明の第１の実施形態の暗号化伝送システムの構成を示すブロック図である。

【図２】　図１から一方向の送受信に関するブロックのみを抜き出した図である。

【図３】　（ａ）は図１の第１通信装置に入力されるパケット信号の送信信

号を時系列に示した図であり、（ｂ）は図１の第１通信装置中の暗号化回路から出力されるパケット信号の暗号化信号ＣＡを時系列に示した図であり、（ｃ）は図１の第２通信装置から出力されるパケット信号の受信信号Ａ’を時系列に示した図である。

【図４】　本発明の第２の実施形態の暗号化伝送システムの構成を示すブロック図である。

【図５】　図４から一方向の送受信に関するブロックのみを抜き出した図である。

【図６】　（ａ）は図５の第１通信装置２から送信されたパケット信号が正常に第２通信装置７に受信される場合のフローチャートであり、（ｂ）は図５の第１通信装置２から送信されたパケット信号に伝送エラーが生じて異常状態で第２通信装置７に受信される場合のフローチャートである。

【図７】　本発明の第３の実施形態の暗号化伝送システムの構成を示すブロック図である。

【図８】　従来の暗号化伝送システムの概略構成を示す図である。

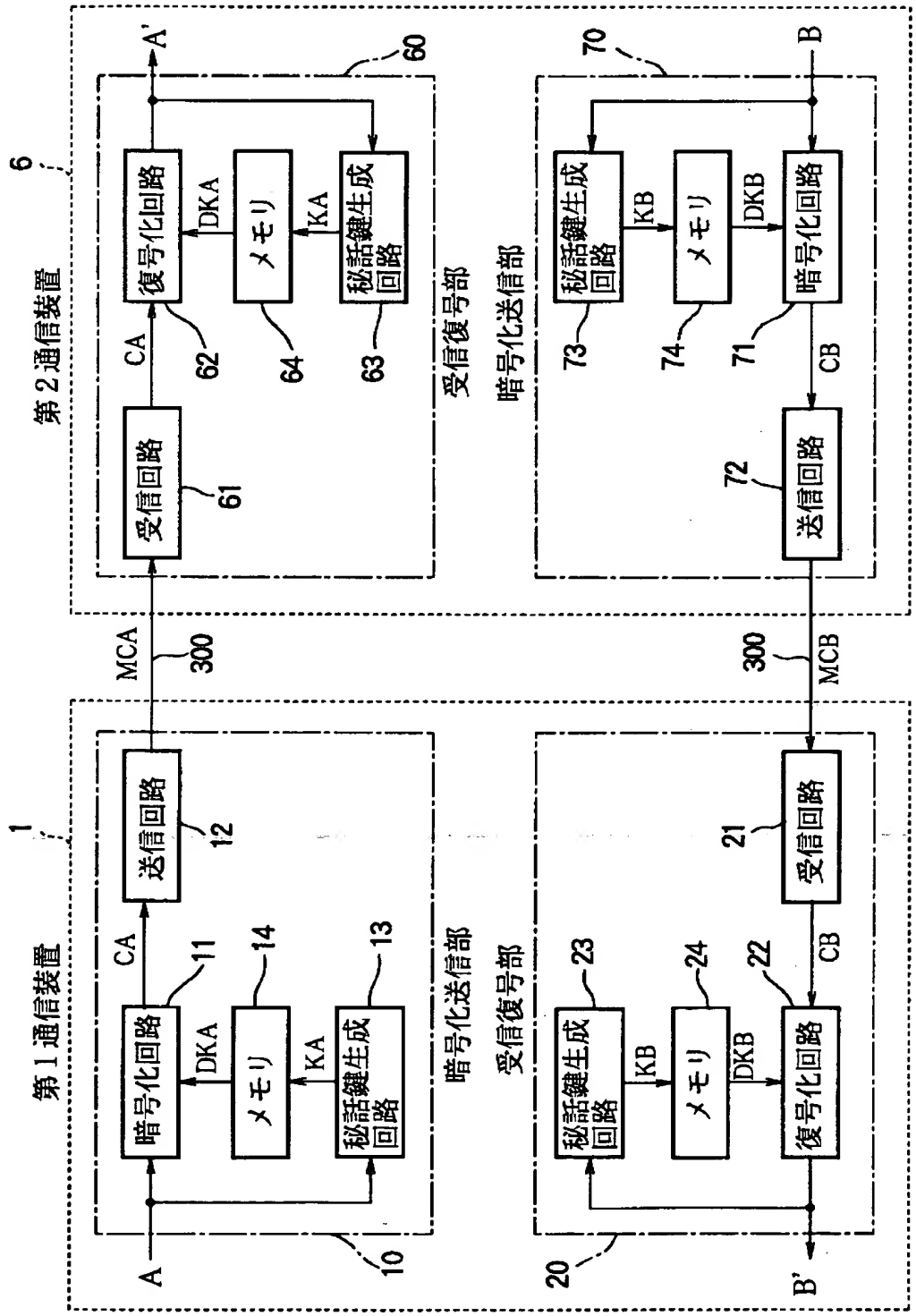
【図９】　従来の暗号化伝送システムの概略構成を示す図である。

【符号の説明】

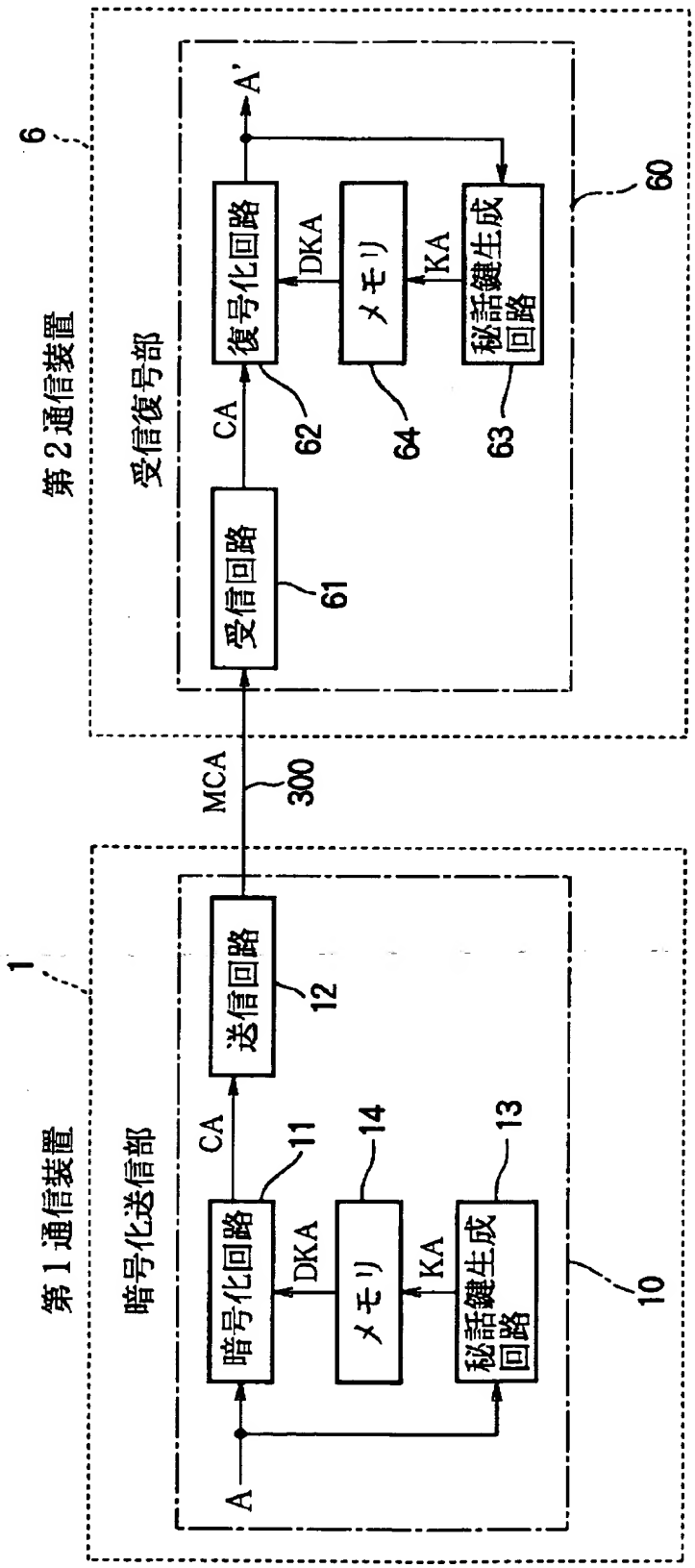
１　第１通信装置、　６　第２通信装置、　１０、７０　暗号化送信部、　２０、６０　受信復号部、　１１、７１　暗号化回路、　１２、７２　送信回路、　１３、２３、６３、７３　秘話鍵生成回路、　１４、２４、６４、７４　メモリ、　２１、６１　受信回路、　２２、６２　復号化回路、　３００　伝送路。

【書類名】　　図面

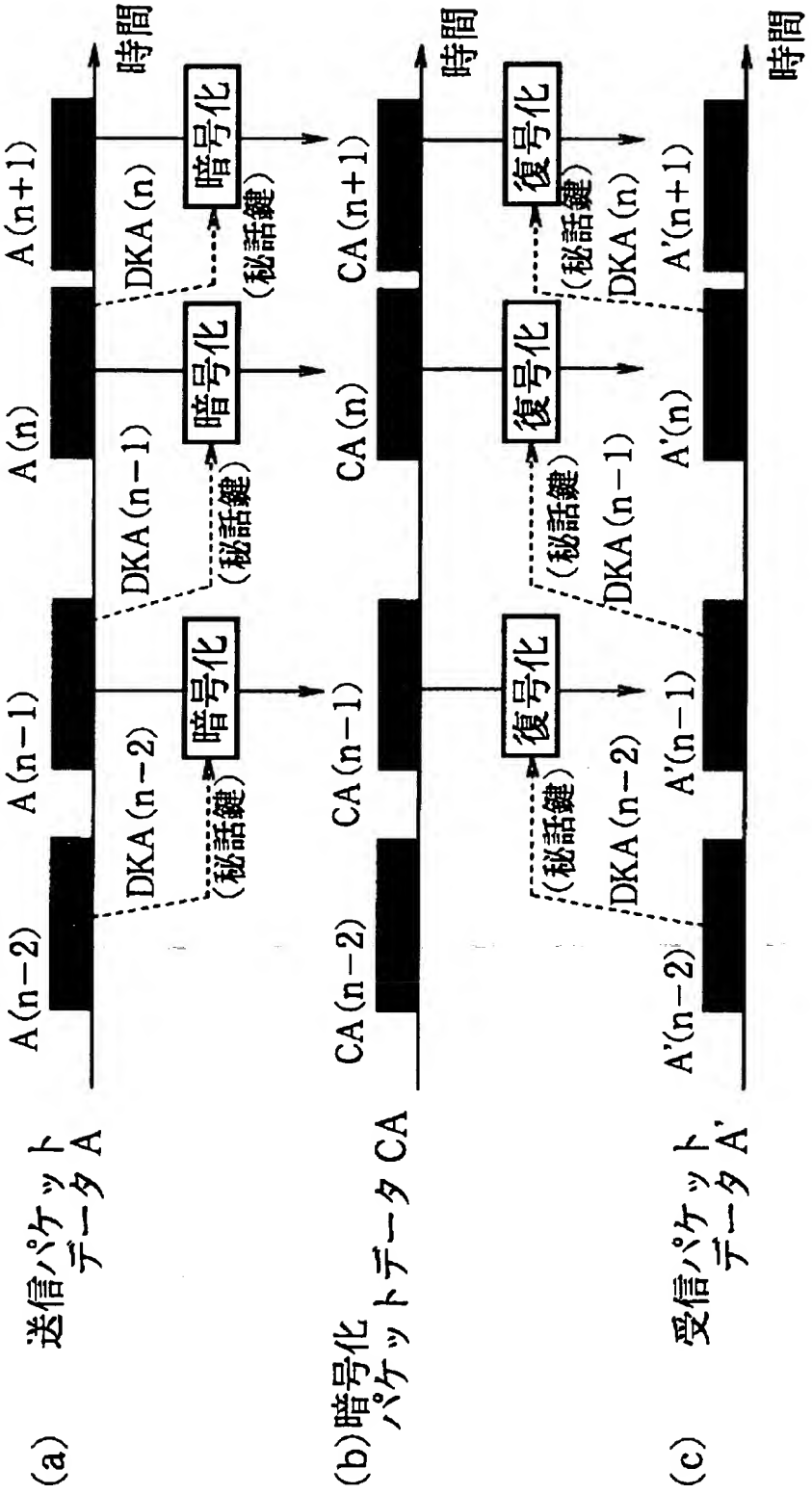
【図１】


第１通信装置
1
第２通信装置
6
暗号化送信部
受信復号部
受信復号部
暗号化送信部
送信回路
12
暗号化回路
11
メモリ
14
秘話鍵生成回路
13
CA
DKA
KA
10
A
受信回路
61
復号化回路
62
メモリ
64
秘話鍵生成回路
63
CA
DKA
KA
60
A'
MCA
300
300
MCB
受信回路
21
復号化回路
22
メモリ
24
秘話鍵生成回路
23
CB
DKB
KB
20
B'
送信回路
72
暗号化回路
71
メモリ
74
秘話鍵生成回路
73
CB
DKB
KB
70
B

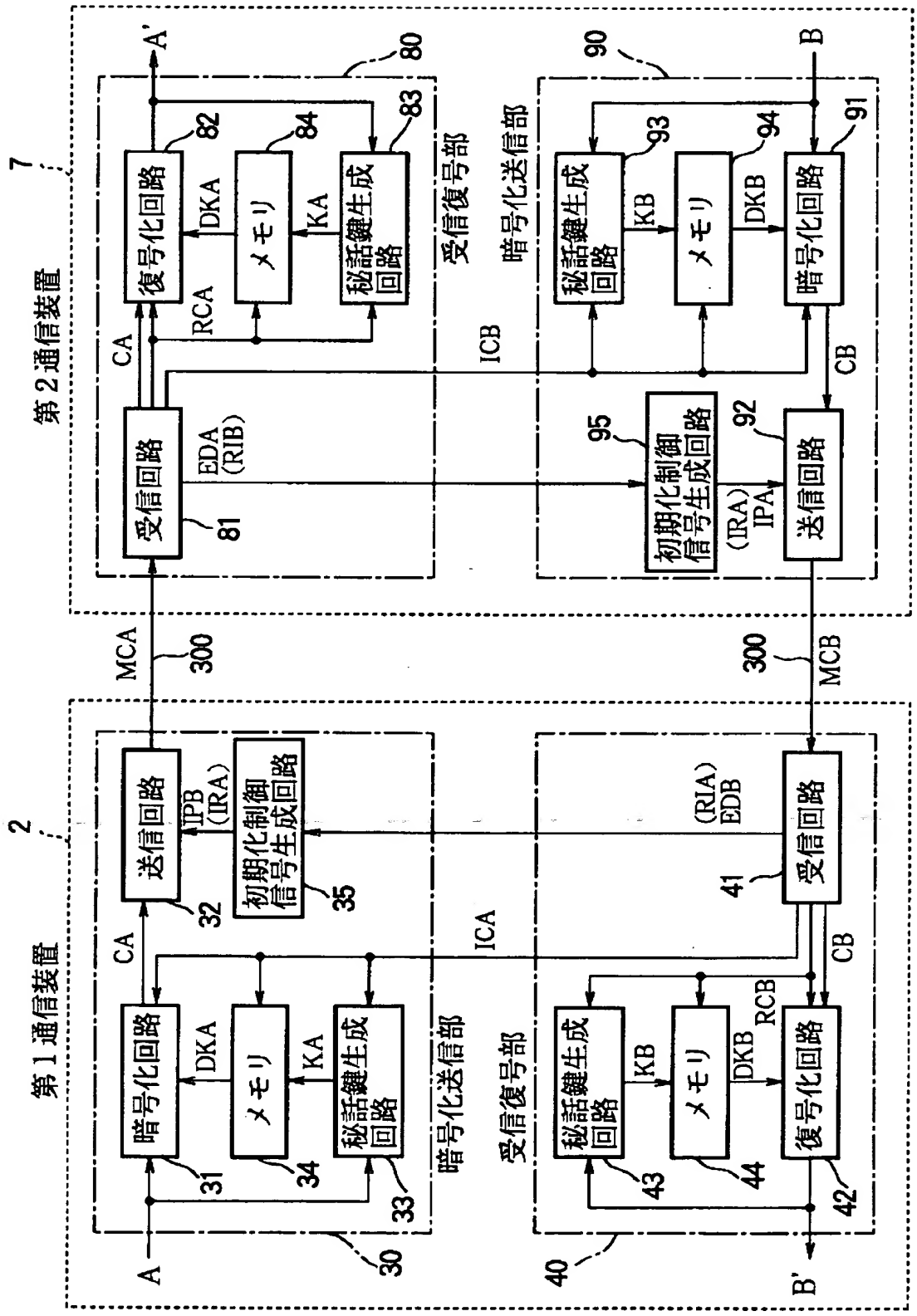
【図２】


第１通信装置
1
暗号化送信部
A
暗号化回路
11
DKA
メモリ
14
KA
秘話鍵生成回路
13
CA
送信回路
12
10
MCA
300
第２通信装置
6
受信復号部
受信回路
61
CA
復号化回路
62
DKA
メモリ
64
KA
秘話鍵生成回路
63
A'
60

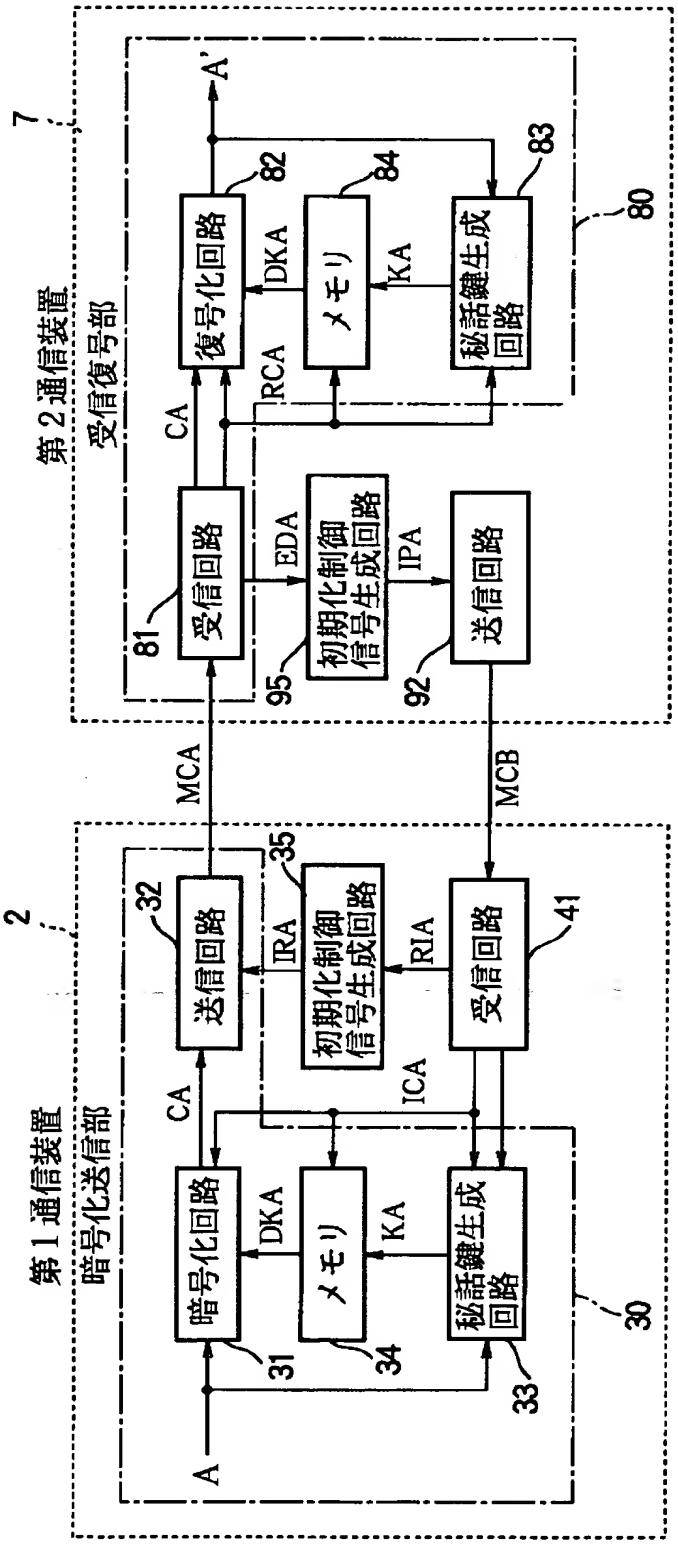
【図３】


(a) 送信パケットデータ A
(b)暗号化パケットデータ CA
(c) 受信パケットデータ A'
時間
A(n-2)
A(n-1)
A(n)
A(n+1)
CA(n-2)
CA(n-1)
CA(n)
CA(n+1)
A'(n-2)
A'(n-1)
A'(n)
A'(n+1)
DKA(n-2)
DKA(n-1)
DKA(n)
(秘話鍵)
暗号化
復号化

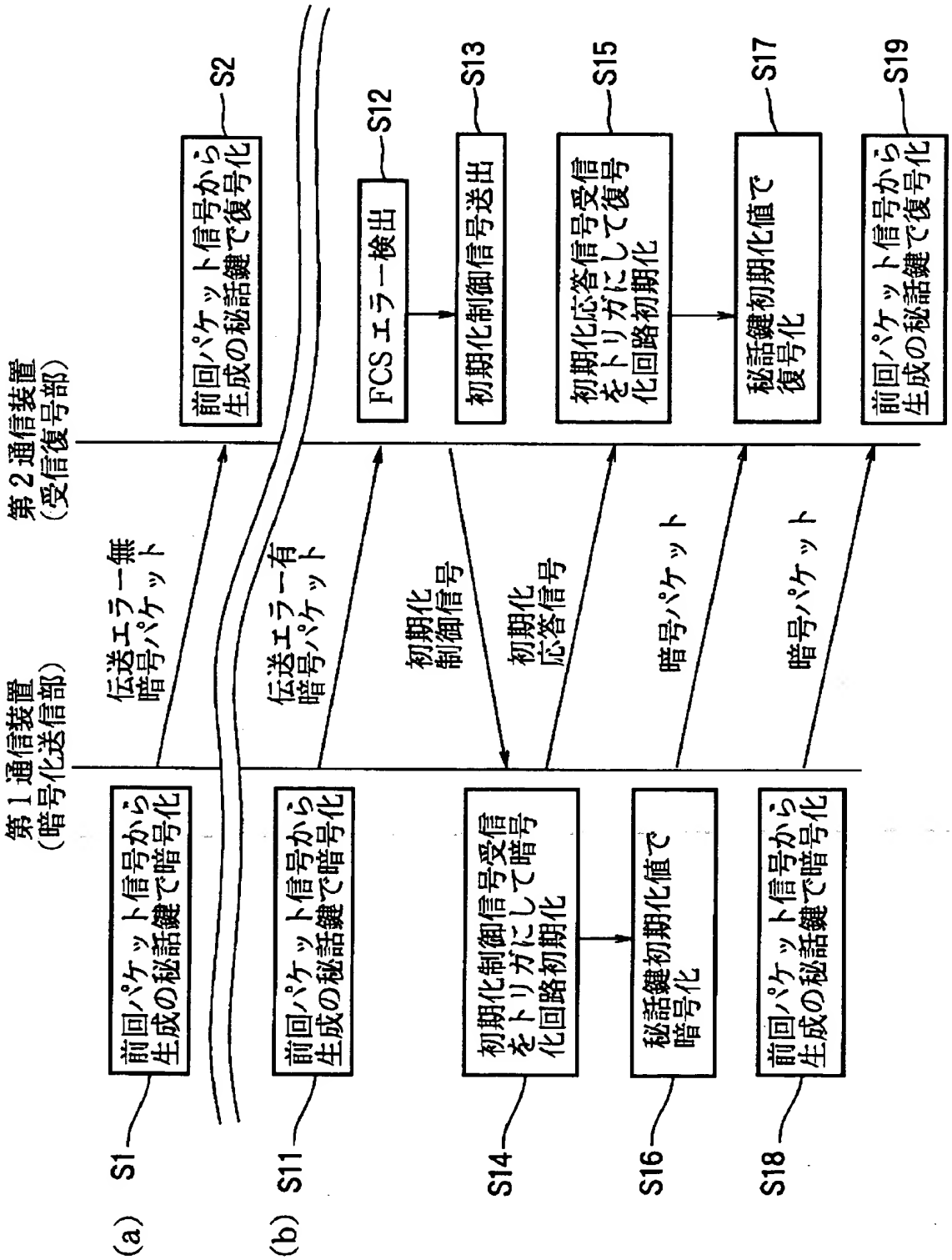
【図４】


第１通信装置
2
第２通信装置
7
暗号化回路
DKA
メモリ
KA
秘話鍵生成回路
送信回路
IPB
(IRA)
初期化制御信号生成回路
CA
ICA
暗号化送信部
受信復号部
A
B'
30
40
31
34
33
32
35
41
42
43
44
復号化回路
RCA
受信回路
EDA
(RIB)
ICB
暗号化送信部
受信復号部
A'
B
80
90
82
84
83
81
91
93
94
95
92
秘話鍵生成回路
KB
メモリ
DKB
暗号化回路
CB
初期化制御信号生成回路
(IRA)
IPA
送信回路
(RIA)
EDB
受信回路
RCB
復号化回路
MCA
300
MCB
300

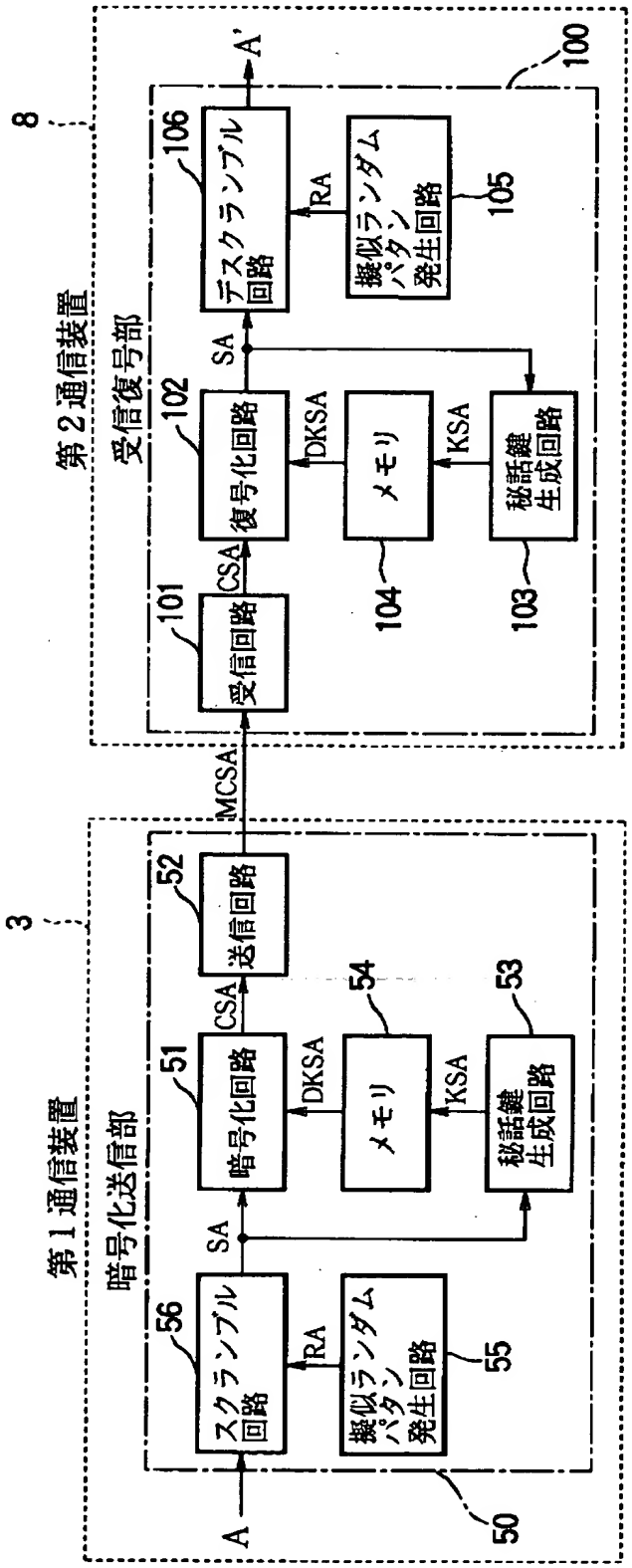
【図５】


第１通信装置
暗号化送信部
2
第２通信装置
受信復号部
7
暗号化回路
メモリ
秘話鍵生成回路
送信回路
初期化制御信号生成回路
受信回路
復号化回路
メモリ
秘話鍵生成回路
受信回路
初期化制御信号生成回路
送信回路
A
A'
MCA
MCB
CA
DKA
KA
ICA
IRA
RIA
RCA
EDA
IPA
30
31
32
33
34
35
41
80
81
82
83
84
92
95

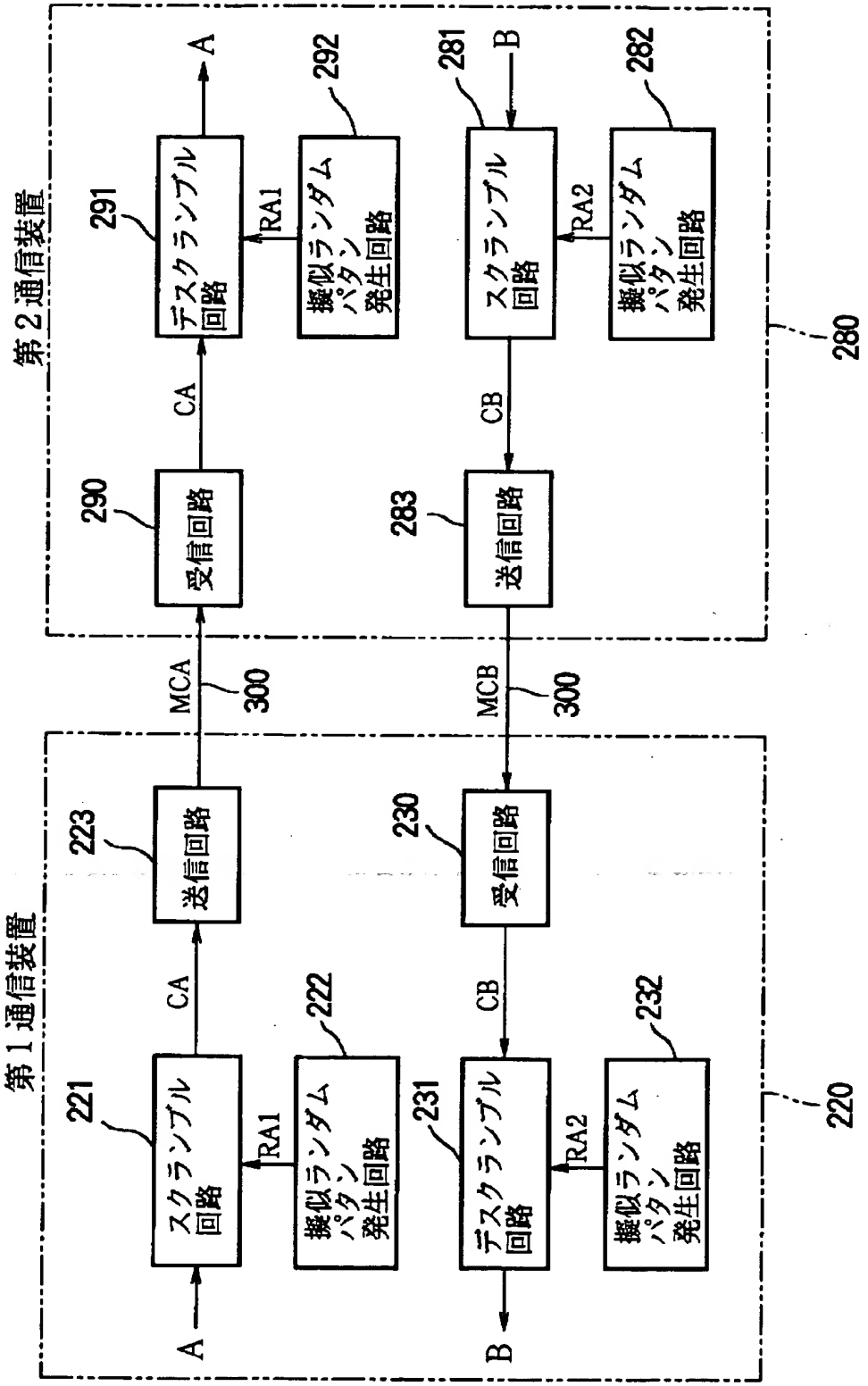
【図６】


第１通信装置
(暗号化送信部)
第２通信装置
(受信復号部)
(a)
S1
前回パケット信号から
生成の秘話鍵で暗号化
伝送エラー無
暗号パケット
S2
前回パケット信号から
生成の秘話鍵で復号化
(b)
S11
前回パケット信号から
生成の秘話鍵で暗号化
伝送エラー有
暗号パケット
S12
FCS エラー検出
S13
初期化制御信号送出
初期化
制御信号
S14
初期化制御信号受信
をトリガにして暗号
化回路初期化
S15
初期化応答信号受信
をトリガにして復号
化回路初期化
初期化
応答信号
S16
秘話鍵初期化値で
暗号化
暗号パケット
S17
秘話鍵初期化値で
復号化
S18
前回パケット信号から
生成の秘話鍵で暗号化
暗号パケット
S19
前回パケット信号から
生成の秘話鍵で復号化

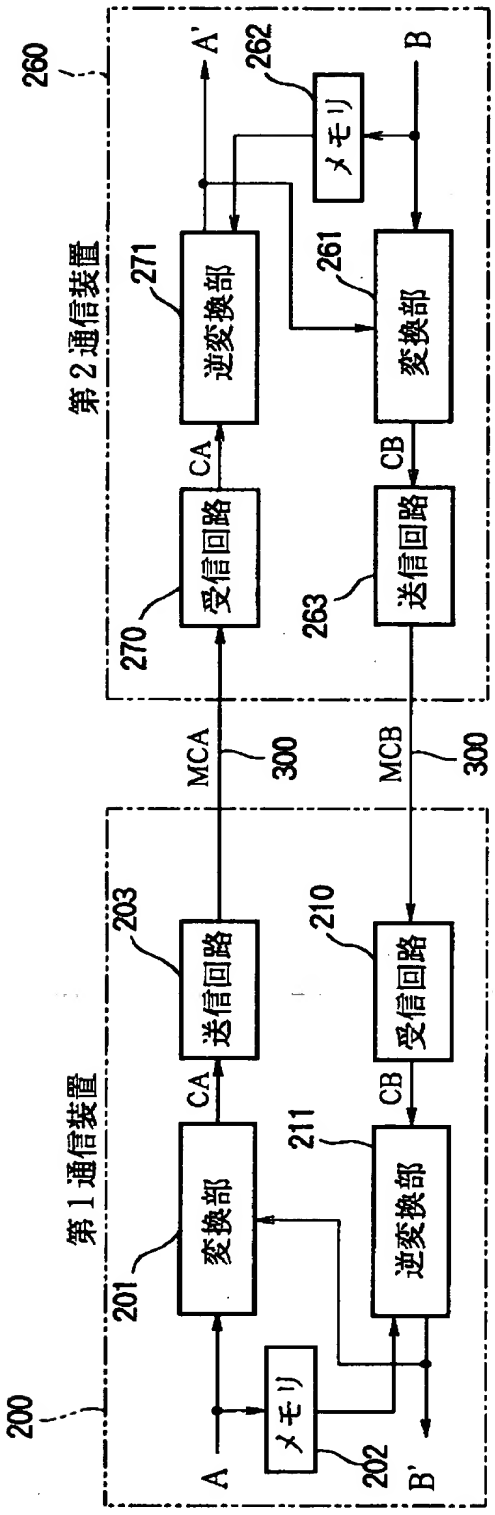
【図７】


第１通信装置
3
暗号化送信部
第２通信装置
8
受信復号部
A
A'
MCSA
CSA
SA
RA
DKSA
KSA
50
51
52
53
54
55
56
100
101
102
103
104
105
106
スクランブル回路
擬似ランダムパタン発生回路
暗号化回路
メモリ
秘話鍵生成回路
送信回路
受信回路
復号化回路
デスクランブル回路

【図８】


第２通信装置
第１通信装置
デスクランブル回路
スクランブル回路
擬似ランダムパタン発生回路
受信回路
送信回路
CA
CB
RA1
RA2
MCA
MCB
A
B
280
220
300
300
290
291
292
281
282
283
230
231
232
221
222
223

【図９】


200
第１通信装置
201
変換部
202
メモリ
203
送信回路
210
受信回路
211
逆変換部
CA
CB
A
B'
MCA
MCB
300
300
260
第２通信装置
270
受信回路
271
逆変換部
262
メモリ
261
変換部
263
送信回路
CA
CB
A'
B

【書類名】　　要約書

【要約】

【課題】　パケット伝送のような間欠的にデータが流れる伝送経路でも暗号化した通信を実施できる簡単な構成の暗号化伝送システムを提供する。

【解決手段】　第１通信装置１は、暗号化前の第１の間欠信号Ａに基づいて第２の間欠信号用の送信側秘話鍵ＫＡを生成する送信側秘話鍵生成回路１３と、送信側秘話鍵ＫＡを第２の間欠信号の暗号化に用いるために遅延させる送信側メモリ１４と、暗号化回路１１とを備え、間欠信号Ａに対して暗号化を実施して暗号化信号ＣＡ（間欠信号）としてから送信回路１２で送出し、第２通信装置６では、復号化後の第１の間欠信号Ａ’に基づいて第２の間欠信号用の受信側秘話鍵ＫＡを生成する受信側秘話鍵生成回路６３と、受信側秘話鍵ＫＡを第２の間欠信号の暗号化に用いるために遅延させる受信側メモリ６４と、受信回路６１とを備えて、受信した暗号化信号ＣＡを復号化回路６２で復号する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００２９５〕

１．変更年月日　　１９９０年　８月２２日
［変更理由］　新規登録
住　所　　東京都港区虎ノ門１丁目７番１２号
氏　名　　沖電気工業株式会社